Experian UK Fraud and FinCrime Report 2025

Trends and tactics on the frontline of fraud prevention and financial crime compliance

experian

Contents

Foreword

Holding the frontline against fraud and financial crime is proving an increasingly expensive endeavour for UK businesses in 2025.

From banks and fintech firms to retailers and telecom providers, most organisations expect to spend more than ever this year on countering criminals and proving to regulators that they are serious about anti-money laundering and sanctions. Just one in 10 expect to claw back budgets in these areas.

At the same time, 59% of businesses tell us that fraud losses continue to mount year on year. A record 421,000 cases were logged on the National Fraud Database in 2024, and generative artificial intelligence (gen AI) appears to be the big enabler, fuelling spikes last year in identity fraud and account takeovers.

How are anti-fraud and financial crime teams fighting back? Do consumers still feel confident about conducting activities online and what do they think of industry efforts to protect them? For the 2025 Experian Fraud and FinCrime Report, we put questions such as these to more than 200 businesses and more than 2,000 consumers across the UK. Their answers provide insights on the progress made so far and where further opportunities lie to cut off the criminals, cut costs and boost consumer confidence.

By highlighting how businesses and consumers are responding to the latest fraud and financial crime tactics, we aim to be part of the fightback, helping you shape next-generation defence strategies that will protect your business and customers.

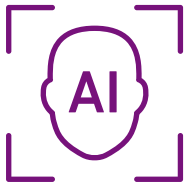
Paul Weathersby,
Chief Product Officer,
Identity & Fraud

of businesses tell us that fraud losses continue to mount year on year

were logged on the National Fraud Database in 2024

experian.

Key takeaways from this year's research



There's no respite in the anti-fraud war as **AI attacks** and counter-attacks proliferate

APP fraud and transactional payment fraud remain the main events encountered by businesses, and we're seeing methods of identity theft and account takeovers

Gen Z are now more anxious about being online than the Baby Boomers

A huge spike in **SIM swapping** underscores the importance of a multilayered authentication strategy

Businesses are trying to improve **AML compliance cost-effectively**, but they're still fighting financial crime in the dark

1 No respite in anti-fraud war as AI attacks and counter-attacks proliferate

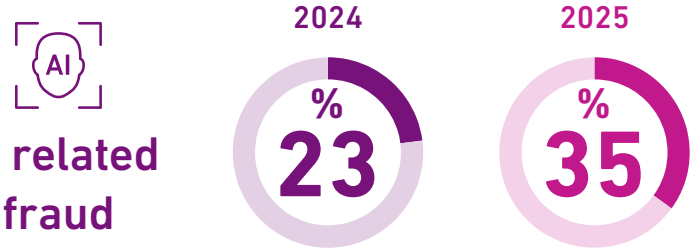
The hyper-convincing alternate reality being generated by generative artificial intelligence (gen AI) is having very real consequences for UK businesses in 2025.

From deepfake footage and cloned voices to synthetic identities and forged official documents, the technology's fabrications continue to supercharge the tactics of international crime groups while lowering the technical barrier for lone bad actors.

Deepfakes are being applied to camera feeds in real time, fooling human observers and biometric authentication systems alike. And gen AI is empowering criminals in distant countries to forge coercive emotional connections with UK consumers.

Just 23% of businesses told us they knowingly encountered gen AI related fraud in 2024, but within the first few months of 2025, this had jumped to 35%.

AI related fraud



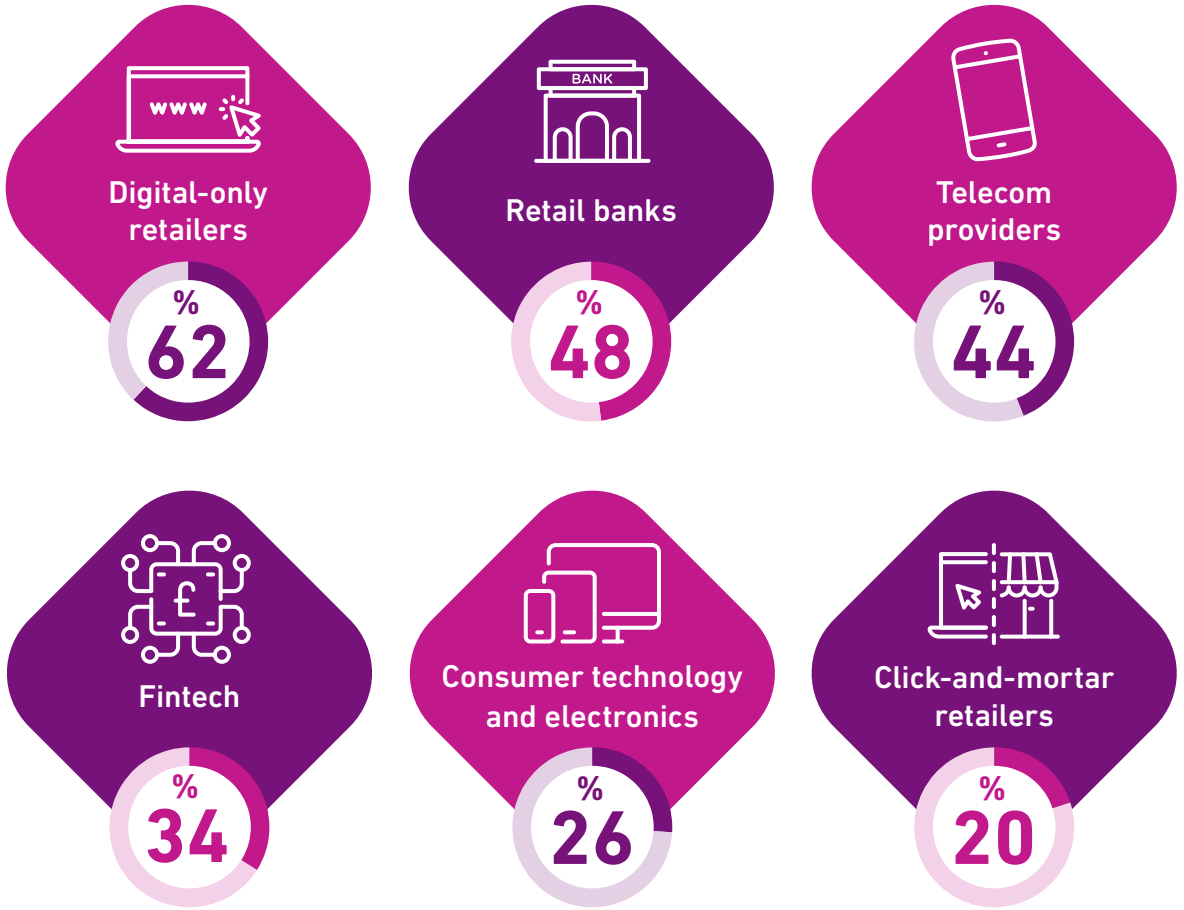
The percentage of retail banks affected has more than doubled from one in five in 2024 to almost half in Q1 2025. Our data shows that digital-only retailers are also at the sharp end of the threat, as are telecom providers.

At the same time, businesses are sharpening their own AI weapons, combining the powers of machine learning and gen AI to stop fraudsters in their tracks. We're seeing an accelerated shift away from rule-based systems and manual processes towards sophisticated and automated technologies that can monitor millions of transactions simultaneously. The most advanced can detect unusual behaviour patterns and assign risk scores in milliseconds, all while reducing false positives and identifying emerging tactics through continuous learning.

One credit card company recently doubled its detection rate of compromised cards by deploying gen AI to match card numbers flagged for suspicious activity with redacted card details advertised on the dark web.

Gen AI is also streamlining some of the burdensome tasks for fraud and financial crime management teams through automated case prioritisation, adverse media monitoring and report generation.

Businesses affected by gen-AI-related fraud in Q1 2025



Are businesses more confident about tackling the AI threat?

It's no surprise that the rapid proliferation of gen AI-powered fraud has knocked business confidence. Back in 2022, this technology was a footnote in fraud risk reports, and 83% of businesses told us they were confident about accurately and consistently identifying customers online. After warnings of deepfake attacks proliferated in 2023, only 68% felt the same.

In 2025, the figure rebounded to 75%, suggesting businesses are regaining their composure, having put robust defences and protocols in place. Malicious gen AI is now firmly public enemy number one, but also an ally helping them fight fire with fire.

More than half (52%) of businesses told us they were implementing and improving AI analytics methods in 2025, and 51% are building new models to improve customer decisions. However, our mirror survey in the US suggests that businesses there are ahead of the UK on proactive AI-powered defences and have bigger fraud budgets.

UK takes proactive, tech-led approach to fraud risk

68% of UK businesses will increase fraud budgets in 2025

64% of UK Tier 1 businesses are planning to implement and improve AI models to improve customer decisions

Anti-fraud investment priorities for 2025

Unsurprisingly, investment priorities for UK fraud teams are aligned with major headaches in the marketplace.

60% are focused on improving detection and prevention of **first-party fraud**

58% are focused on improving detection and prevention of **synthetic identity fraud**

56% are focused on improving detection and prevention of **APP fraud**

2 Same old deceptions – new methods and motives

Little has changed in the last three years when it comes to the types of fraud most commonly encountered by businesses. What keeps changing is the modus operandi and sophistication of the fraudsters and, in the case of consumer perpetrators, their motives.

The most common fraud types encountered by organisations in 2024

APP fraud, money mules and scams

Our survey found that scammers who trick victims into willingly sending them money are considered the top operational challenge for businesses in the next two to three years. Now that payment system providers are legally required to reimburse most consumer victims of authorised push payment (APP) fraud, the stakes are higher than ever – and gen AI is raising them.

At the extreme end is the UK engineering firm where an employee was tricked into transferring £20 million to criminals after they roped him into a video call with deepfakes of the company's Chief Financial Officer and other staff members.

On a more routine basis, we're now seeing fraudulent call centres exploiting voice cloning technology to talk to victims in whatever accent is likely to win their trust. Meanwhile, online romance scammers are using deepfake technology to present themselves in whatever guise will be considered classically attractive by their targets.

However, UK businesses appear to be making headway in preventing these crimes. Romance scams, investment scams and purchase scams – whereby a victim pays in advance for goods or services that never turn up – all declined in the first half of 2024. Cases in which criminals pose as a bank or the police and persuade people to transfer money to a "safe account" have also fallen, suggesting that bank communication campaigns warning about this scam are getting through to consumers.

Money muling still going under the radar

Consumers remain less switched on to the risk of being recruited by criminals to launder the proceeds of crime. Just one in eight UK consumers expressed concern to us this year about 'money muling', whereby individuals are paid to receive money and then forward it to criminal accounts, whether knowingly or unknowingly. Acting as an intermediary for criminal gangs can be a devastating experience for ordinary people, whereas the real perpetrators often remain untraceable.

Worryingly, among those consumers concerned about money muling, 13% admit to having acted as a money mule, while 29% say a friend, family member or acquaintance has done it, with young people twice as likely to be targeted as older groups.

Transactional payment fraud

Fraudsters continued to exploit weaknesses in online payment processes to hijack the process. With mobile wallets and retail apps growing in popularity, criminals are honing phishing tactics and the realism of spoof websites and fake apps to seize card credentials and personal information.

In one scam exploiting the Government's cuts to the winter fuel allowance, con artists reach out on social media or through text messages and direct people to what looks like an official website set up to help them cut their bills. They then trick victims into sharing a one-time passcode (OTP) from their bank, allowing them to set up a digital wallet with the victim's card details.

Identity theft

Affecting more than one in three businesses in 2024, identity theft is the number one source of stress impacting anti-fraud teams this year. After a short reprieve, the crime is back in our top five of most commonly encountered fraudulent events due to the double whammy of major security breaches and gen AI-assisted tactics convincing people to hand over personal information.

However, but it's nature, we must also consider synthetic identity theft, whereby ID data is being used to adapt and create synthetics. Whilst it may have dropped out of the top five this year, synthetic identity theft still a significant threat to UK financial institutions, costing them more than £300 million a year in losses.

The ease with which gen AI can concoct convincing personas to sit alongside the stolen personal details of real people is clearly at the top of mind for businesses. Six in 10 are prioritising investment in tackling synthetic ID fraud in 2025, and 55% intend to increase investment, making this a key growth area. Click-n-mortar businesses, in particular, are ramping up investment. One contributory factor may be increased age and ID proofing required through upcoming legislation around the sale of knives online.

One emerging cybercrime tactic is the 'repeater', whereby fraudsters use subtly varied deepfake-enhanced synthetic identities to quietly test a financial institution's digital defences multiple times before exploiting its weak spot in a full-blown attack. Despite challenges such as these, most businesses (78%) told us they were confident they could address synthetic ID fraud.

Account takeover

Back in the top five fraud types encountered by businesses in our survey, account takeover was a major problem for telecom providers in 2024 as unauthorised SIM swaps soared by more than 1,000%. (See Chapter 4). The scam enables fraudsters to take control of victims' mobile phone numbers and intercept two-factor authentication codes to take over sensitive accounts. Depending on the type of website or app they access, they might apply for a bank loan, cancel holidays to get a refund or even steal wages from gig economy workers.

First-party fraud

First-party fraud shot up in 2022 when the cost-of-living crisis blurred the lines between cynical criminal activity and deception as a way to survive genuine hardship. Since then, pressures on households have eased somewhat. However, payment service providers steeled themselves for another spike in first-party fraud in October after the Payment Systems Regulator's (PSR) rules came into effect, requiring them to reimburse consumer victims of authorised push payment (APP) scams in all but exceptional cases.

Their concern was that consumers would play the victim to elicit a payout for APP scams that they orchestrated themselves or in which they were complicit. It is no surprise then that first-party fraud is back in the top five most common fraud events, and its prevention tops the list of investment priorities for businesses, with 60% actively pursuing or planning to engage in this area.

3 Gen Z and Millennials now more concerned than Boomers about being online

Online anxiety is a growing consumer trend this year, but one big surprise is the increased concern among younger generations.

The oldest cohort in our research (age 55-69) have long expressed worries about conducting activities online, aware that their age group is a prime target for scammers.

But, in stark contrast to last year, Gen Zs and Millennials are more concerned about being online these days than the Boomers, according to our research (52% and 49% vs 45%, respectively). This is no subtle ambivalence. The proportion of "very concerned" consumers aged 18-24 has nearly tripled from 5% last year to 14% now, and for consumers aged 25-39, it has more than doubled to 17% from 7% last year.

In contrast, only 7% of people over 40 feel "very concerned" about conducting activities on the internet, although this too is a jump up from 4% in 2023.

Unlike the older generation, whose main worry is identity theft, phishing and scams, Gen Zs are anxious mainly about online privacy and misinformation. This digitally native generation has grown up liberally sharing their photos and locations through social media channels such as TikTok and Snapchat. But now, with deepfakes routinely appearing on social media, they seem to feel more vulnerable to fake news and false advertising.

Interestingly, younger people profess to be less aware of online scams than their elders. They feel just as targeted by fraudsters as older people but have less expectation that businesses would reimburse them for any fraud losses.

This uncertainty may explain why consumers of all ages increasingly prize online security and privacy over convenience, even though 84% of businesses are committed to reducing customer friction when implementing fraud defences.

Top 3 concerns by age group

	18–24	25–39	40–54	55–69
1	Online privacy	Online privacy	Identity theft	Identity theft
2	False information & fake news	Theft of credit card information	Online privacy	Online privacy
3	Theft of credit card information	Identity theft and scams or phishing	Theft of credit card information	Scams or phishing

Affluent feel more targeted but also more protected

People on high incomes feel more concerned about conducting activities online than those on low incomes, but they are also more aware of industry efforts to protect them from fraudsters.

Customer opinion

Income level

100%

"I feel more of a target for online fraud than I did 12 months ago"

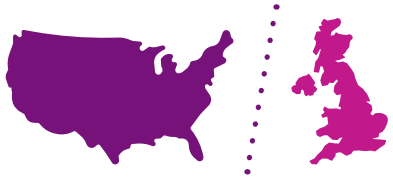
- Low 32%
- Medium 34%
- High 53%

"I believe that businesses have put more security procedures in place over the past 12 months"

- Low 44%
- Medium 51%
- High 72%

"I feel safer using biometric security features (face or fingerprint authentication) more now than I did 12 months ago"

- Low 47%
- Medium 55%
- High 70%



Atlantic digital divide:

Our US survey shows that consumers across the Pond are more digitally engaged and comfortable sharing data, whereas UK consumers prioritise trust, clarity and stability in digital experiences. Brits also have higher expectations around transparency and accountability, leaning more towards traditional authentication methods, though this is likely to change with greater awareness of defences such as behavioural biometrics.

4 Identity crisis: SIM swapping surge underscores the importance of a diverse authentication arsenal

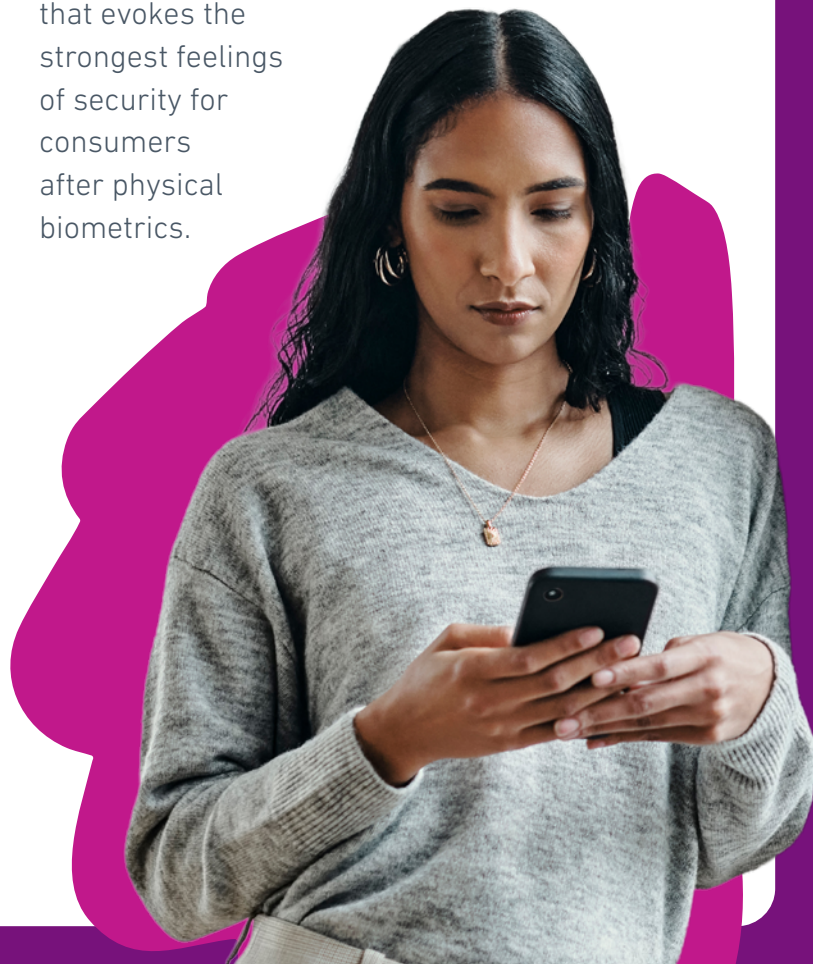
A massive spike in 'SIM swapping' fraud has dealt a crushing blow to any UK business still reliant on two-factor authentication in 2025.

Nearly 3,000 unauthorised SIM swaps – whereby criminals hijack someone's mobile phone number by transferring it to a new SIM card under their control – were logged on the National Fraud Database in 2024. That's an increase of more than 1,000% on 2023 when only 289 instances were recorded.

The tactic starts with fraudsters gathering personal information through phishing and social engineering or data breaches, such as those resulting from the recent cyberattacks on UK-based international retailers. They then contact the victim's mobile provider, posing as the customer, and request a SIM swap, often citing a lost or stolen phone. Once in control of the number, criminals can intercept one-time passcodes sent via SMS to take over the victim's accounts. Depending on the websites or apps they can access, they might apply for a bank loan, cancel holidays to get a refund or even steal wages from gig economy workers. Far from a one-off event, the scam gives them repeated access with enduring consequences. Even after the SIM is recovered, fraudsters may have already planted backdoors such as password resets and linked devices or harvested sensitive data to sell on the dark web.

It's a stark reminder for consumers not to overshare personal details online. However, for businesses, the implications are complex. SIM swapping combines identity theft and cybercrime – the two biggest causes of increased stress for businesses in 2024, according to our research.

The scam illustrates the ease with which fraudsters can now intercept PIN codes sent to mobile devices – the customer authentication method that evokes the strongest feelings of security for consumers after physical biometrics.



We are reassured to see that businesses are investing more heavily on multi-factor authentication defences such as knowledge questions, secondary devices and physical and behavioural biometrics, as well as multimodal tools that can check credentials in different formats including text, image, audio and video.

As we've seen time and time again, any authentication method that seems failsafe will not stay failsafe for long as criminals develop new ways around it. It's vital that businesses build multilayered authentication arsenals and stay vigilant to emerging threats such as quantum hacking.

The benefits of biometrics

Enhanced security
Biometrics, whether fingerprint scans, facial recognition, or behavioural patterns, provide a unique identifier that is much harder to forge, or steal compared to passwords or PINs.

Reduced fraud risk
Since biometrics rely on physical and behavioural traits unique to an individual, the likelihood of identity theft or unauthorised access is significantly lower.

Improved user experience
Biometrics eliminate the need for complex passwords, making authentication more seamless and convenient for users.

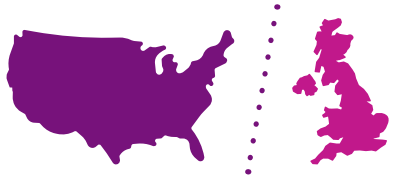
Real-time fraud detection
Behavioural biometrics can analyse patterns in user interactions, detecting anomalies in real time to prevent fraudulent transactions before they happen.

Minimised false positives
Combining biometrics data with traditional fraud detection capability, can provide a far more comprehensive view of risk whilst also reducing false alerts.

Authentication methods that evoke the strongest feelings of security in consumers*

*Among consumers who had encountered these methods in the past six months, the percentage who rated them as "extremely secure" or "very secure".

** via SMS, email or app notification



Atlantic digital divide:

US consumers have more confidence in discreet authentication methods

34% of US consumers vs 31% of UK consumers are aware of behavioural biometrics as an identity authentication method.

Consumers awareness of behavioural biometrics

US	UK
% 34	% 31

Among those aware of behavioural biometrics, 94% of US consumers are confident in the method vs 54% of UK consumers.

Consumers confidence in behavioural biometrics

US	UK
% 94	% 54

5 Businesses strive for cost-effective AML compliance – but they're still fighting FinCrime in the dark

Failure to comply with anti-money laundering (AML) and sanctions regulations cost some big banks dearly in 2024 – but compliance, too, is coming at a high cost for UK businesses.

Fines imposed by the Financial Conduct Authority (FCA) tripled to a record £176 million last year as regulators sought to stem the flow through financial and professional services firms of criminal funds that threaten national security and prosperity.

More than one in four businesses in our survey were fined for non-compliance with AML regulations in 2024, including 38% of retail banks.

Despite the scrutiny, this appears to be less of a priority area for most businesses than fraud prevention and detection – perhaps because of its insidious nature. Money laundering and the other financial crimes it underpins are estimated to strip 14.5% from the UK's gross domestic product, undermining the integrity of the entire financial system. But most businesses acknowledge that they don't "completely understand" its impact on their organisation.

The compliance imperative, however, is inescapable and means that 57% of businesses will increase their AML budget in 2025.

Emerging strategies for cutting AML compliance costs

Machine learning models that can spot patterns in vast datasets offer tantalising potential for money laundering detection and even prediction. One in five businesses is already using the technology for just that and we expect to see this rise in the coming years. However, many of the processes involved in AML compliance require human judgment and oversight. So, it's not surprising that staffing costs are high in the tightened regulatory environment.

As businesses battle to comply cost-effectively, we can see two key strategies emerging:

1 Improving detection

65% are investing or actively planning to invest in prevention by improving detection of financial crime at the onboarding stage.

By catching bad actors before they enter the system, they can avoid the costly complications of exiting the customer, reporting suspicious activity and potentially being fined.

Bringing teams together 2

60% are focused on improving how they bring siloed fraud and AML teams together into more comprehensive FRAML (fraud and anti-money laundering) functions, continuing a trend we saw last year.

By ensuring financial crime red flags and fraud alerts are seen by the same team, they can detect suspicious activity better and reduce duplication of effort.

Government should close the AML intelligence loop

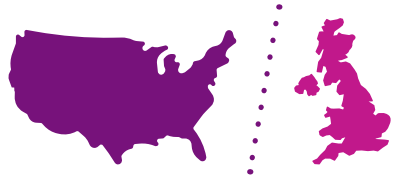
Data-sharing within organisations through integrated FRAML teams is a positive trend in financial crime management. We applaud the Economic Crime and Corporate Transparency Act, which took effect in 2024, making it easier for AML-regulated organisations to share customer data with each other for prevention, detection and investigation.

However, there's a critical missing link in the financial crime data-sharing chain that only the Government can close. Currently, just 1% of investigations by businesses result in a suspicious activity report (SAR) to the National Crime Agency. And although 30% of UK businesses tell us they filed at least one SAR last year; we estimate that only 1% of these resulted in a conviction. Until organisations have insight into which red flag in 10,000 is a genuine case of financial crime, they're unlikely to make a dent in the illicit finances flowing through the financial system. Indeed, the mounting false positive rate will only push up costs further, disincentivising cooperation.

We recommend the Government establishes a structured prosecution outcome database. With backing from industry and the leveraging of ML models to detect patterns in the data, businesses could stop fighting financial crime in the dark and start scaling up effective vetting and prediction.

of UK businesses tell us they filed at least one SAR last year

we estimate that **only 1%** of these resulted in a conviction



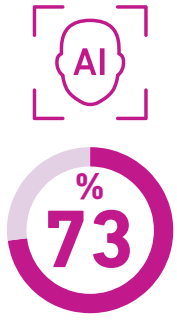
Atlantic digital divide:

UK more focused on money laundering

57% of UK businesses vs 32% of US businesses anticipate their AML budget will increase in 2025.

Businesses who anticipate their AML budget will increase

73% UK Tier 1 businesses are planning to implement and improve AI models to improve customer decisions.



6 How can Experian help?

Gain a unified view of fraud risks and act fast

Our integrated platform delivers real-time fraud alerts while ensuring a smooth, secure experience for legitimate customers. With our rich data and analytics, you can reduce fraud and streamline onboarding.

Stay ahead with real-time fraud prevention tech

Prepare for regulatory changes and outpace fraudsters with our advanced analytics, data, and software. We helps organisations detect and stop fraud in real time, across all sectors.

Leverage machine learning for smarter fraud detection

CrossCore, our fraud platform, uses built-in ML to spot emerging threats early and reduce costs. It's scalable and accessible for businesses of all sizes.

Empower customers to protect themselves

Use our consumer insights to understand customer behaviour and knowledge gaps. Educate them on online safety and fraud risks to build resilience and reduce vulnerability.

Strengthen KYB with robust data verification

Unlike unverified sources, we use over 20 data points to validate business customers. Our multi-source approach uncovers hidden risks and provides a clearer picture of company structures.

Build trust through secure, reliable interactions

Strong authentication and fraud prevention foster trust. Demonstrating your commitment to security helps deepen customer relationships and protect your brand.

Combine fraud and AML strategies for stronger protection

Our solutions support both fraud and AML teams with shared insights and analytics. This integrated approach enhances compliance and risk management throughout the customer lifecycle.

Conclusion

As businesses navigate the dual pressures of rising fraud losses and escalating consumer expectations, the need for robust and adaptive fraud management strategies has never been greater.

The data highlights a clear trend: consumers demand seamless yet secure digital experiences, and businesses are responding with increased investments in advanced fraud prevention technologies.

The rise in fraud types such as APP fraud, transactional payment fraud, and identity theft underscores the urgency for businesses to adopt comprehensive, multilayered fraud management solutions. With the anticipated growth in fraud management budgets in 2024, the emphasis will be on integrating cutting-edge technologies like generative AI, physical and behavioural biometrics, and machine learning to stay ahead of increasingly sophisticated fraud tactics.

Experian's suite of solutions, including the CrossCore platform, offers a powerful toolkit for organisations to combat fraud effectively. By leveraging our advanced analytics, real-time data insights, and integrated fraud detection capabilities, businesses can not only mitigate fraud risks but also enhance customer trust and streamline their onboarding processes.

In an era where the digital landscape is continually evolving, maintaining a proactive stance on fraud prevention is essential.

To learn more about how Experian can support your fraud prevention efforts, visit our website or contact us to discuss your specific needs. Let us help you build a safer, more trustworthy digital environment for your customers.

Organisations prioritising a holistic approach to fraud and financial crime management will be better equipped to protect their customers and sustain their operations in a secure and compliant manner.

About the Experian research (methodology)

The Experian UK Fraud and FinCrime Report 2025 is based on two major surveys, conducted in the UK. The first asked more than 2,000 UK consumers about their online interactions and their expectations with regards to security and customer experience. The second survey asked more than 200 UK businesses about their strategies for effective fraud and AML management, as well as customer identification and authentication, including investments in new security and customer-experience-related technology solutions. Organisations surveyed for the research include retail banks, fintech organisations, digital retailers, electronics providers, payment providers and many other companies from a range of verticals.

Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

www.experian.co.uk/business